

# Hardware Designs for Secure Microarchitectures

Jan Philipp Thoma, Ruhr University Bochum

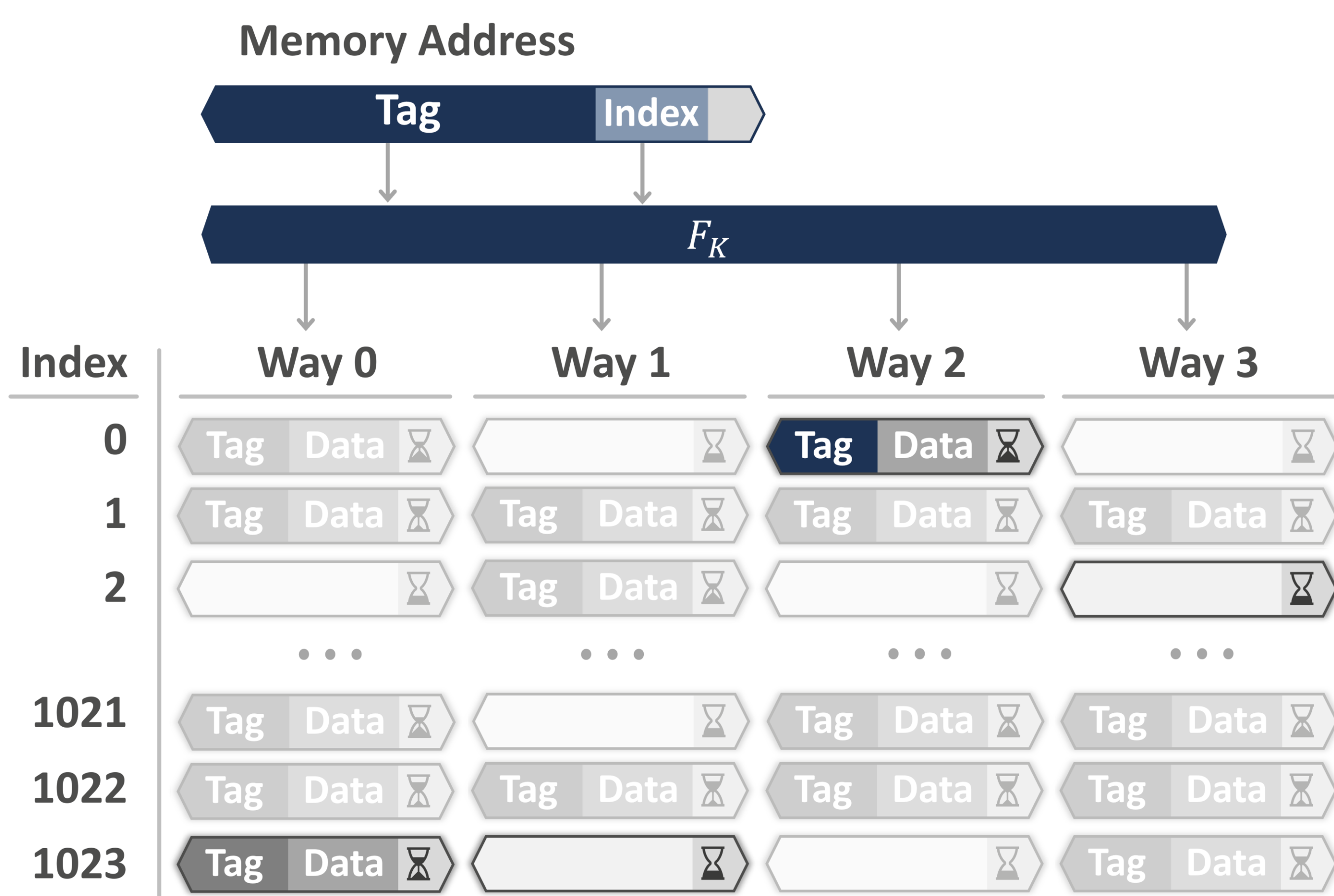
## Overview

### Topics:

- Cache attacks and countermeasures
- Transient execution attacks
- **7 (+1) publications** in peer-reviewed conferences and journals, including 2x USENIX Security
- A **new side channel** in Intel CPUs (RAID 2022)
- Side-channel **secure cache** and **TLB** architectures (USENIX Security 2023, TCHES 2023/1)
- Secure and efficient implementation of **randomized caches** (USENIX Security 2023, AsiaCCS 2024)
- Hardware-based cache **attack detection** (Submitted)
- Reducing the performance dependency of modern processors on **speculative execution** (RAID 2021, DATE 2024)

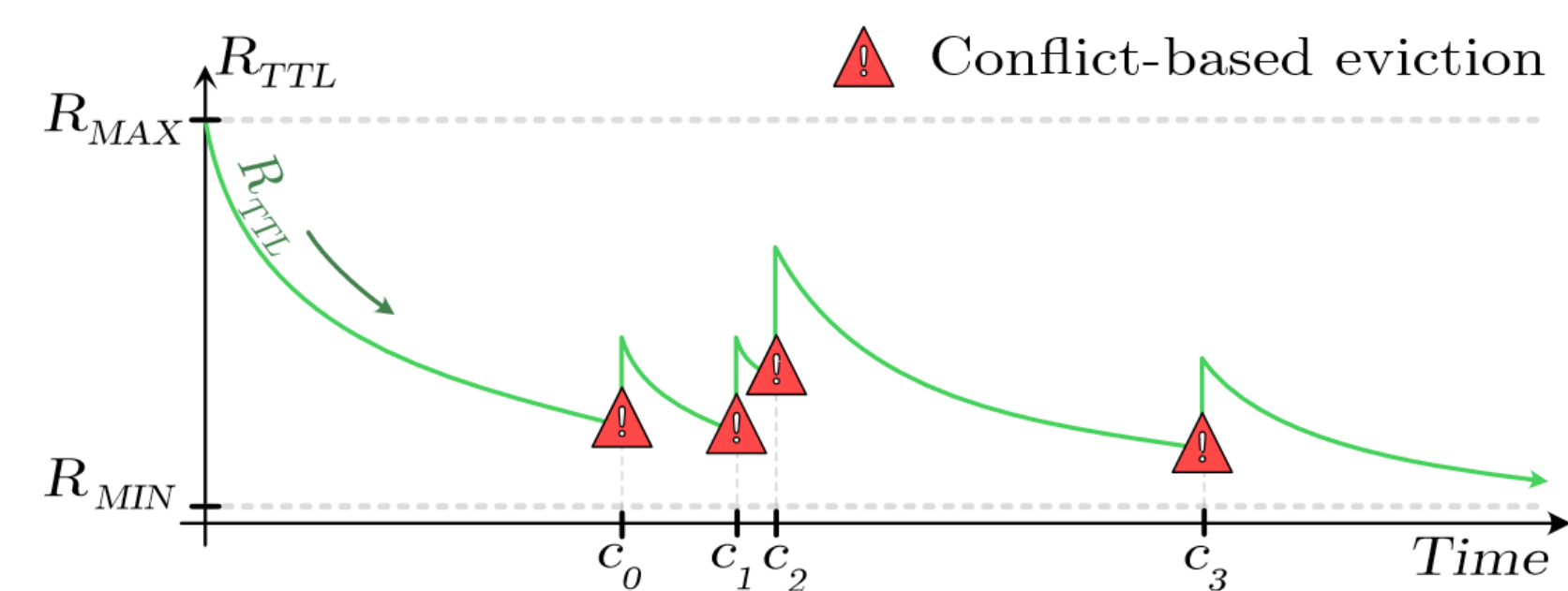
THESIS

## ClepsydraCache



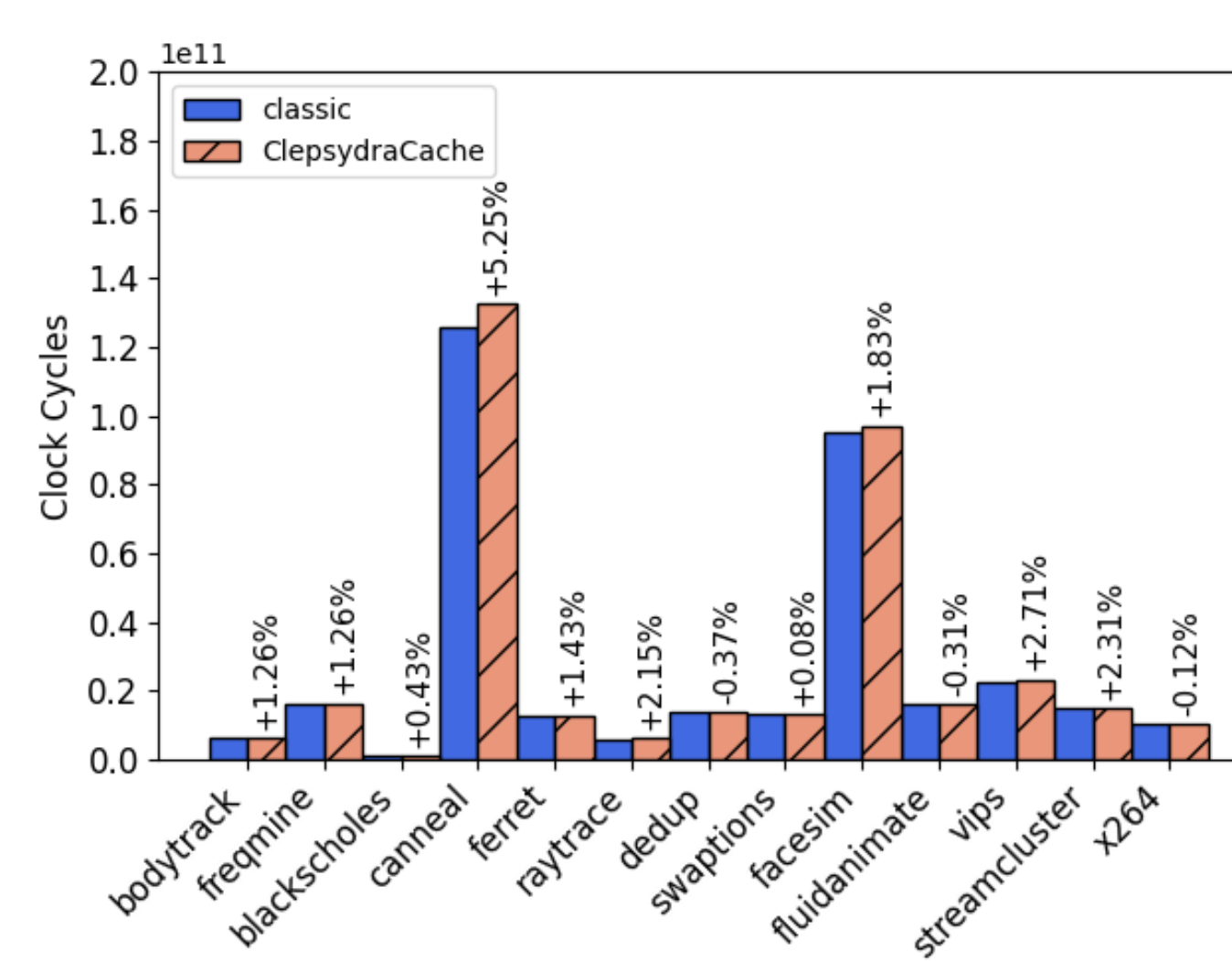
- Side-channel secure cache architecture based on **decay** and **randomization**
- Dynamic scheduling of the **time-to-live (TTL)**
- **Capacity-based implementation** of TTL
- Empty entries and time-based evictions make ClepsydraCache secure against **Prime+Prune+Probe** attackers
- Performance overhead between **-0.37%** and **+5.25%**

## TTL Scheduling

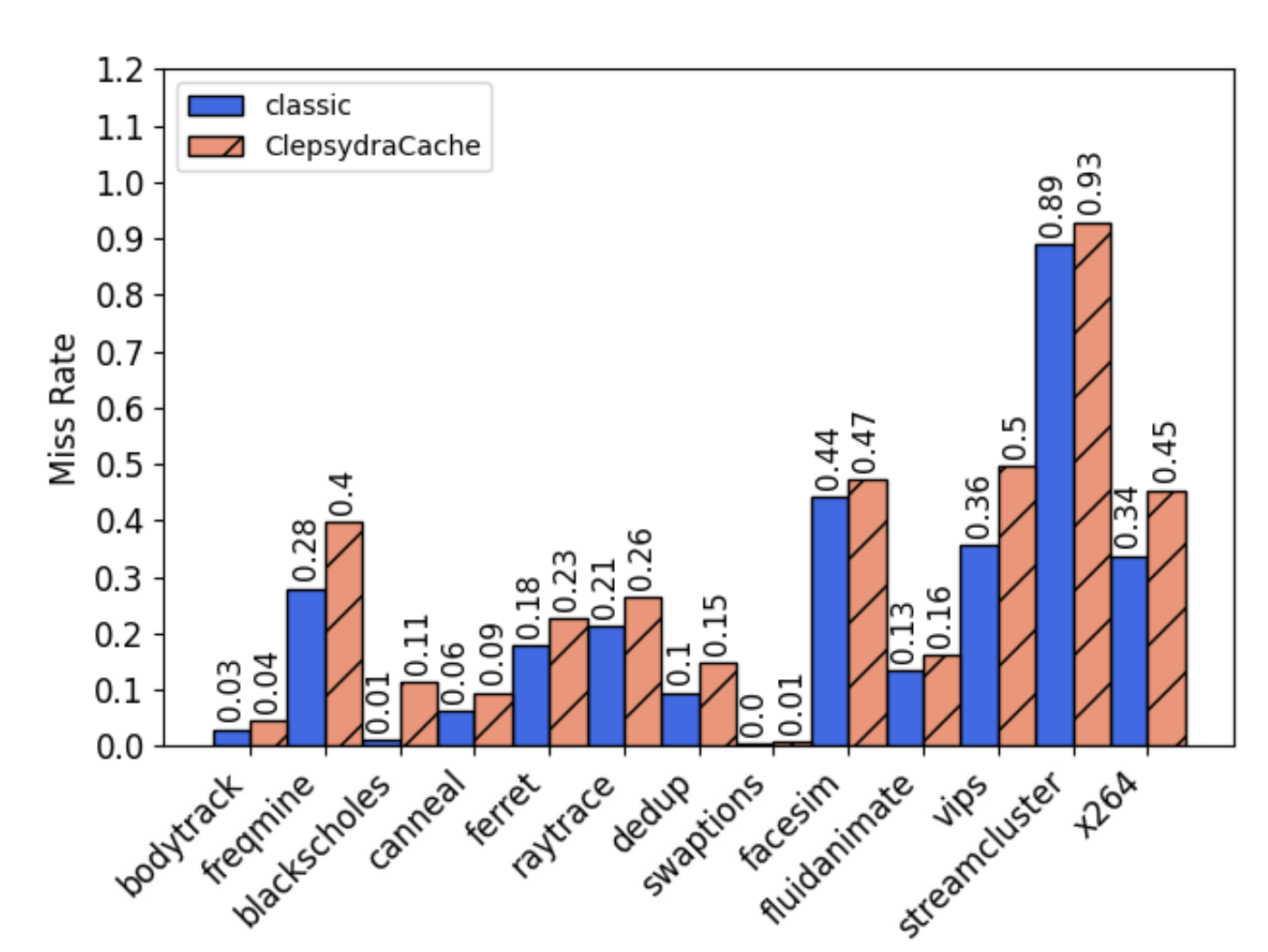


- TTL is dynamically scheduled based on cache activity
- Many conflicts  $\rightarrow$  faster eviction based on TTL
- Few conflicts  $\rightarrow$  longer lifetime of entries

## Performance



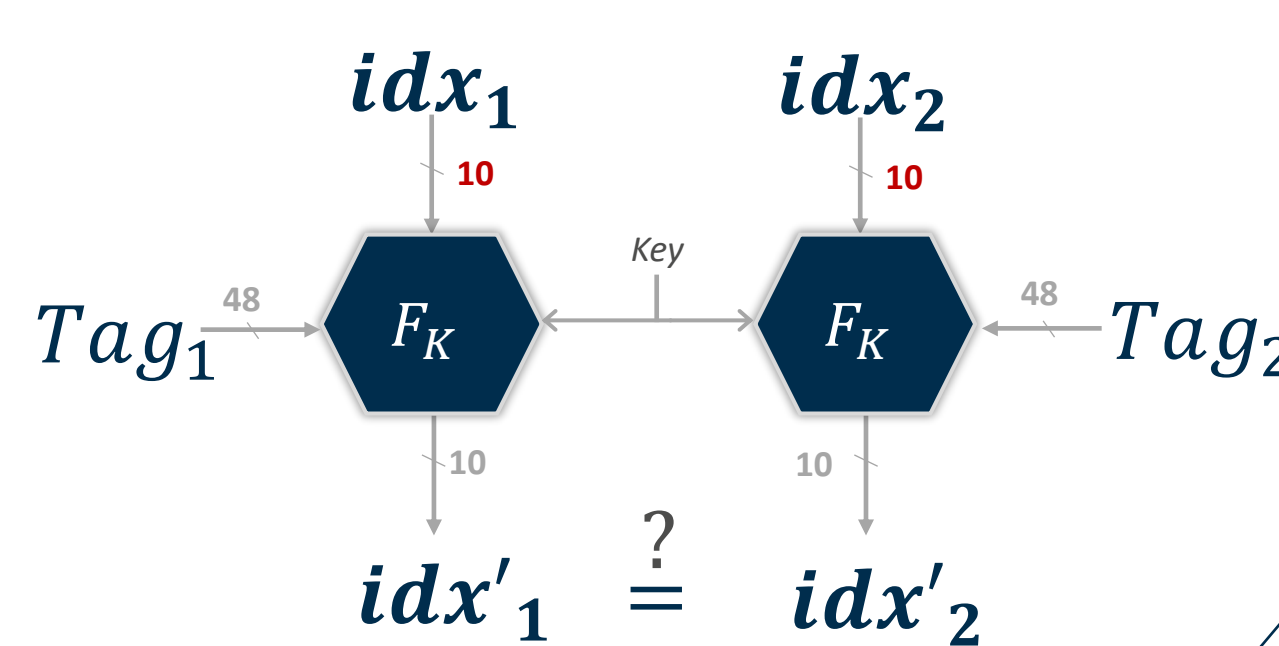
## Cache Miss Rate



## SCARF

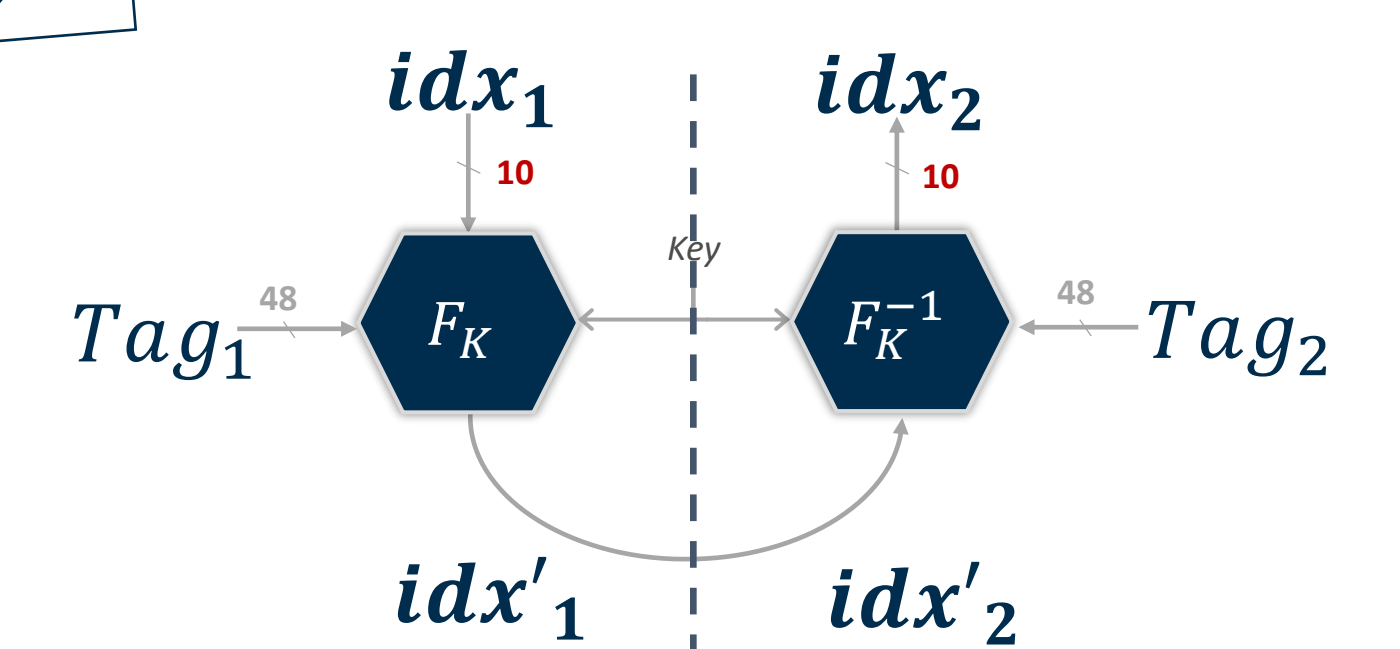
- Secure Cache Randomization Function
  - **Low latency**
  - **Key dependency**
  - **Invertibility** (given the tag)

### Attacker's View



- Attacker learns if two addresses collide
- Does not learn  $idx'$

### Designer's View



- Design a secure function in the design view
- Half the number of rounds

